

Solution Overview



REAL ID

REAL ID: WHERE WILL IT LEAD US?

*A Whitepaper by:
Nathan Root, Manager, and Harold Kocken, Manager,
BearingPoint's National Motor Vehicle Practice*

The Real ID Act

The Act signed into law on May 11, 2005 requires states to adopt minimum federal standards for the issuance of driver licenses and personal identification cards. States must also modify any conflicting laws or regulations in order for their documents to be recognized by federal agencies for official purposes.

In a report published on September 21, 2006, the National Governors Association (NGA), the National Conference of State Legislatures (NCSL) and the American Association of Motor Vehicle Administrators (AAMVA) gave an initial cost estimate for implementation of Real ID at over \$11 billion. This report and its bottom line cost estimate brings to light the impact Real ID implementation will have on the states.

The Real ID Act requires not only a reassessment of the current business practices of the motor vehicle community, but a reassessment of the complete business environment. The Act is compelling states to leverage existing systems and integrate new applications to enable new or modified business processes that were previously unthinkable because of their cost and perceived impacts upon customer service.

Alternative Legislation

Senators Daniel Akaka (D-HI) and John Sununu (R-NH) introduced Senate Bill 4117, the Identification Security Enhancement Act of 2006, shortly before the closing of the 109th Congress. The bill would repeal the Real ID Act and reinstitute Section 7212 of the *Intelligence Reform*

and Terrorism Prevention Act of 2004. Key aspects of the proposed bill would:

- Provide states with additional regulatory flexibility
- Include funding authorization to more rapidly produce tamper- and counterfeit-resistant driver licenses
- Incorporate protections for privacy and civil liberties included through a negotiated rulemaking process

In his remarks on the floor introducing the bill, Senator Akaka indicated their intention for the alternative legislation. The intention is to wait for the Notice of Proposed Rulemaking (NPRM) from the Department of Homeland Security (DHS) for Real ID to determine whether or not to pursue any action on S. 4117. The "wait and see" approach insures a protracted period of uncertainty surrounding the Real ID requirements.

The Rules

Although the Real ID Act was passed in May of 2005, the DHS has yet to publish the rules for the Act that will provide a better understanding of what it will take to implement Real ID. This extended timeframe for development of the rulemaking is indicative of a relatively new federal agency addressing a complex business and a politically volatile community of stakeholders. It took the U.S. Department of Transportation six years to implement the Commercial Motor Vehicle Safety Act of 1986 requiring states to adhere to minimum standards for licensing commercial drivers by April 1, 1992. The DHS is being asked to implement minimum document issuance standards for all drivers in only three years.

Timeline

Because of the estimated cost impact of the Act, DHS is required to send the draft rulemaking with a cost/benefit analysis to the Office of Management and Budget (OMB) for review and approval. OMB will have up to 90 days to perform the review and request feedback from other federal

agencies. DHS will also have to consult with the White House on the rulemaking draft as part of the OMB process. It is anticipated that DHS will need more time to amend the rulemaking based upon OMB's response to the initial draft. In a best case scenario, the rulemaking will be published as a Notice of Proposed Rulemaking (NPRM) in the Federal Register by April/May 2007. Many comments are expected to be submitted, further influencing the time DHS will need to analyze and address the comments and to amend the rulemaking. The Final Rule will be published no sooner than August 2007, leaving states less than 10 months to implement. The recently introduced bill S4117 may have even further impact on the rulemaking being prepared further delaying the process of publishing rules.

Biggest Areas of Impact

Re-enrollment. As the NGA /NCSL /AAMVA report indicates, the most significant impact of Real ID will be the re-enrollment process. There are approximately 245 million people with valid driver licenses and ID documents. Real ID will require all 245 million document holders to present themselves in person and comply with new Real ID processes that will be more time consuming than previous document issuance procedures. Citizens will have to find documents (e.g. social security card, birth certificate and immigration documents) they may not have seen in years and present them at the DMV in person. They will also have to make sure that their names on the different documents match or that there is sufficient evidence on why a name has changed over time. The procedures that DMVs will have to implement to comply with the Act will put a heavy burden on the citizens. This is compounded by a potentially short timeframe – DHS may begin enforcing Real ID for air travel and other purposes as early as May 2008. DHS initially indicated that all current holders should be re-credentialed within five years. Even if the re-enrollment period is extended to ten

years the cost would only be marginally lowered as all 245 million holders would still have to be re-credentialed. Two additional significant impact areas are included within the new enrollment procedures: digital imaging of source documents, and verification systems for the source documents.

Digital imaging. As part of the new credentialing process states will have to digitally image and store all source documents used to verify the identity of the applicant. Many states do not currently have a document imaging system. Those that have an imaging system originally implemented the systems under different conditions to support smaller applications, and the imaging systems were not integrated with the state's driver license or identity management system. Real ID requires image capture, storage, and retrieval for source identity documents for all driver license and ID card holders throughout the state. On average each customer will have between three and five documents whose images need to be captured and stored. This means that approximately one billion images will have to be captured and stored for all current card holders, in a way that will allow easy retrieval. Citizens may have a hard time finding the correct official documents and may face repeated visits to the DMV to complete the process of providing proof of identity. The distributed nature of the requirement, combined with the greatly increased volume of images, adds up to a need for robust and scaleable document imaging and content management systems.

Verification systems. Each state is unique in the way they do business and that also holds true to the documents they accept for identification purposes. There are, however, a number of documents that are commonly accepted in the identity environment. These documents are:

- Social security cards
- Passports
- U.S. birth certificates

- Immigration documents
- Military credentials
- State issued driver's licenses and identification cards

DHS has indicated that at the core of their new issuance process they will require verification of the information contained in these "breeder documents" by going to the issuing authority to verify that it actually issued the document to a person with the information provided. For instance, states will be required to check U.S. passports with the Department of State, Social Security Numbers with the Social Security Administration and U.S. birth certificates with the vital records agency of the state that issued the certificate. Currently only two systems are operational for use by motor vehicle agencies (Social Security Online Verification – SSOLV and the Systematic Alien Verification of Entitlement). Both federal agencies responsible for these systems (Social Security Administration and DHS/United States Citizenship and Immigration Services) are working on enhancing their respective systems to support the increased demand and additional business requirements resulting from the Real ID Act.

Other verification systems contemplated by DHS for required verification are not fully deployed on a national scale. DHS is working with the state vital records agencies through the National Association for Public Health Statistics and Information Systems (NAPHSIS) to encourage all state vital records agencies to become connected through a system called the Electronic Verification of Vital Events (EVVE). This system would allow the verification of birth and death record information (if available electronically). The vast majority of states currently are not connected through EVVE and do not have their vital records available in a format that allows electronic verification of the records. Driver license verification is operational only for commercial

licenses, accounting for only about 13 million of the 245 million current card holders. Building systems and the individual state interfaces to support the requirement DHS envisions will be a major undertaking, especially converting the current records for legacy identity documents (such as birth and death records) to a format that can be electronically retrieved and checked, as well as the sending of images of source documents.

The re-enrollment, digital imaging and verification requirements constitute the biggest impacts of Real ID. They highlight some of the most critical changes states will have to undertake in their organizational structure and business processes.

Privacy and Civil Liberties

The pending Real ID rulemaking and advancing technology will require motor vehicle agencies (MVAs) to re-assess the availability of information, from personal information to public information. Existing state and federal laws and regulations (e.g. the Driver Privacy Protection Act (DPPA)) will have to be reviewed and updated to assure that privacy and civil liberties are protected appropriately. The Real ID Act of 2005 itself does not directly address privacy, a concern that was expressed by senator Akaka when introducing the Identification Security Enhancement Act of 2006 (S4117).

There are a number of initiatives ongoing by federal agencies that indicate privacy has become more important. The U.S. Social Security Administration (SSA) is proposing to revise its privacy and disclosure rules to clarify certain provisions and to provide expanded regulatory support for new and existing responsibilities and functions. These changes in the regulations will increase agency efficiency and ensure consistency in the implementation of the SSA's policies and responsibilities under the DPPA and the Social Security Act. SSA's efforts will impact the

requirements for participation in SSOLV. The E-Government Act of 2002 recognized that these advances also have important ramifications for the protection of personal information contained in government records and systems. The E-Government Act mandates an assessment of the privacy impact of any substantially revised or new information technology systems. The document that results from these mandated assessments is called a Privacy Impact Assessment (PIA). The DHS Privacy Office has performed several of these PIAs on DHS programs and recently published the results.

Privacy principles, also known as fair information practices, should form the basis of every MVA's codes and policies like we see in many industry codes and policies. In the early 1970's the U.S. Department of Health and Human Services first developed eight privacy principles that have become the basic principles many organizations adhere to.

These eight principles are:

- **Openness.** The public should be informed of the existence of all systems and databases that are being established.
- **Collection limitation.** Only collect the information necessary for your business purpose.
- **Data quality.** All data is kept "accurate, complete, current and verified."
- **Individual participation.** Each individual has the right to:
 - Examine the data kept on himself or herself
 - Request corrections to be made in case of errors
- **Use limitation.** Clearly defining the use of personal information being collected; developing strict adherence to the defined use; and providing criminal penalties for misuse.
- **Disclosure limitation.** Clearly defining who has access to personal information.
- **Security.** Personal data should be protected from dissemination by built-in safeguards

against loss, destruction, tampering, theft and unauthorized use or disclosure.

- **Accountability.** Providing a mechanism to assure that privacy principles are met and adhered to and that violations will be addressed appropriately.

Fully understanding the importance of these principles and the need to adhere to them within the motor vehicle environment where sensitive personal information is gathered will be an important task for MVAs. This personal information will become even more sensitive with the oncoming Real ID requirements that will put more emphasis on the gathering of personal information and its use. Break ins and thefts of computers and other equipment containing sensitive personal data have occurred in recent months and years at MVAs across the country – these occurrences provide proof of the urgency and importance of protecting personal information to the fullest. Aside from establishing more complete and accurate repositories of personal identity information in each MVA, the Real ID requirement to perform an “all jurisdiction look up” in particular will require strict observance and implementation of privacy rules.

Adherence to the privacy principles and developing a process supporting them can be beneficial to the MVAs. A key principle is that of “individual participation.” Having a process in place where the customer can verify his or her personal information available in the motor vehicle record and is able to make changes to the information does not only make the MVA compliant with this privacy principle, but will help the MVA to clean up the information in their system and diminish the impact of bad data when the customer comes to the office to go through the Real ID compliant process.

Future of Issuance Requirements under Real ID

There are a number of federal laws and programs that over time may affect driver licensing. The main laws and programs are:

- Western Hemisphere Travel initiative
- Transportation Worker Identification Credential
- Federal Worker Employee Credential (HSPD-12 / PIV)
- Trusted Traveler Initiative
- E-passport and E-pass card

DHS is involved in all of these areas and will have looked at spheres of commonality to assure avoiding duplicate efforts and looking for best practices that can be used when developing the rulemaking for Real ID. Although biometric and smart card solutions probably will not be part of Real ID rulemaking, DHS will have seriously considered them in the process. The impact these technologies will have on the current motor vehicle environment, coupled with the additional cost estimates for implementing them and the public's apparent unease with these technologies, make them unlikely candidates in the short term. However, this will change over the long term. As technology advances, the price will come down and more and more people will become familiar with these technologies so that the obstacles for using them in the motor vehicle community will diminish.

These technologies can help increase productivity, efficiency and security, and the associated costs are anticipated to decrease. DHS is therefore preparing the current Real ID rulemaking to be a platform for future advancements that will increase the security and quality of the issuance process living up to the premise: *one person – one driver license* – one driver record, both for national security as well as highway safety reasons.

The information that will come from the DHS funded Kentucky Real ID pilot will further define the Real ID requirements. The pilot results may not be available in time for influencing DHS's Final Rule, but its interim results may persuade Congress to extend the May 11, 2008 implementation date.

What Will the Rules Hold in Store?

Assuming that the new political landscape does not pursue S. 4117 to repeal the Real ID Act, and the Act isn't struck down by the judicial branch on Constitutional grounds (such as infringement of Federalism principles), states will have to implement Real ID by May of 2008. DHS has provided some perspective on what the rulemaking may require during meetings of the Real ID State Work Group. This Work Group was comprised of representatives from federal agencies, law enforcement organizations and state-based organizations (NGA, NCSL and AAMVA). DHS recently hinted at a phased approach by creating "safe harbors" as they called it. This phased approach would allow states to comply with a minimum set of requirements by May 11, 2008, requiring full compliance over a more extended period. This phased approach would alleviate some of the burdens faced by the states. The question now is what will be required by May of 2008. The following bullets provide areas we believe DHS will focus on initially:

Real ID Compliance Items	Business Process	Systems Verification	Database	Card Format
Digital image capture and storage ¹	✓		✓	
Verification of social security and immigration information through SSOLV, SAVE.	✓	✓		
Vital record check through Electronic Verification of Vital Events (with possible delayed implementation)	✓	✓		
Driver's license check with all other states.	✓	✓		
Capture of digital photographic image of all applicants.	✓		✓	✓
Capture of "full legal name" up to 175 characters.	✓	✓	✓	
Introduction of the 2-dimensional PDF417 barcode as the common machine readable technology.	✓			✓
Introduction of a performance-based document security scheme that will require a minimum level of protection against a set of security threats (but not requiring a specific substrate and specific security features).	✓			✓
State plans for implementation of security schemes for all document production facilities.	✓		✓ ²	
Real ID compliant indicator on documents issued under the new issuance process and acceptable for official purpose.	✓			✓
Grandfather rule for a set of document holders (In the past, DHS has indicated those born before 1935 and having lived in the state for a minimum of 10 years may be grandfathered). In addition DHS may opt to grandfather other population segments (e.g. federal employees).	✓			
At a minimum require background checks for all new hires.	✓	✓		
Require fraudulent document recognition training for specific employees as determined by the state.	✓			
Update appropriate privacy statutes and policies and perform appropriate Privacy Impact Assessments	✓	✓	✓	✓
Require all DL/ID cards issued on or after May 11, 2008 to have a validity period not exceeding 8 years.	✓			✓
No biometrics required (e.g. fingerprint, iris scan)	✓	✓	✓	

¹ There is a possibility, reading the intent of the Act in the Conference Report, that DHS will not require digital capturing of all source documents and the image of the applicant but just the digital capturing of the image of the applicant in the first phase.

² DHS may require security measures that impact the security of and determines access to the driver record databases in the states.

BearingPoint's Real ID Alliance

BearingPoint has an experienced motor vehicle team that is complemented by a strategic business network. BearingPoint has put together a team of companies and individuals that is uniquely poised to deliver DMV and Real ID expertise to ensure rapid deployment with a minimum of system integration costs. Its expertise even extends back to the time when the Intelligence Reform and Terrorism Prevention Act of 2004 was first introduced. BearingPoint delivers a forward looking solution that is highly scalable and flexible allowing for additional Real ID requirement solutions later on to be seamlessly integrated or amendments to be made based on new legislation.

BearingPoint has teamed up with 3M and IBM (FileNet) to offer states a process automation solution that streamlines document verification and identity authentication while complying with the Real ID Act. The highly configurable and user-friendly design allows for efficient integration into current back-end business. Beyond meeting the requirements of the Act, our solutions will increase operational efficiencies and reduce time and expense related to paper processes. In addition to the basic solutions to Real ID, BearingPoint provides expertise in Project management to help increase overall agency efficiency, reduce costs, and maximize service oriented architecture technologies.

BearingPoint: Management and Technology Consulting for Today's Business Environment

BearingPoint is a leading management and technology consulting company that serves the Global 2000 and many of the world's largest public services organizations. Our experienced



Management & Technology Consultants

professionals help organizations around the world set direction to reach their goals and create enterprise value. By aligning their business processes and information systems, we help our clients gain competitive leadership advantage – delivering results in an accelerated time frame. To learn more, visit our Web site at www.bearingpoint.com or contact:

Gary Miglicco
Vice President, BearingPoint, Inc.
512.542.5301
gary.miglicco@bearingpoint.com

Securities Safe Harbor

With the exception of historical information contained in this release, the matters described herein contain certain "future-looking statements" that are made pursuant to the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995. Such future-looking statements include statements regarding the expected requirements that will be part of the still pending REAL ID Act rulemaking, as well as other statements containing the words "believes," "expects," "will" or words of similar import or statements of management's opinion. These statements are subject to certain assumptions, risks, uncertainties and changes in circumstances. Actual results may vary materially from those expressed or implied from the statements herein or from historical results, due to changes in economic, business, competitive, technological and/or regulatory factors. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect management's opinions only as of the date of this release. Except as required by law, we undertake no obligation to revise or publicly release the results of any revision to these forward-looking statements.